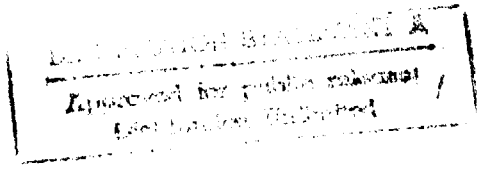
RAND

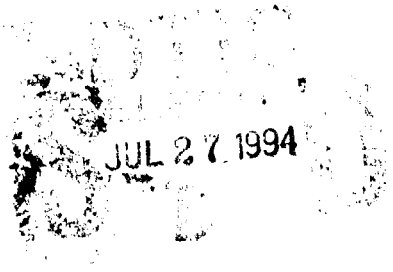
Route Planning Issues for Low Observable Aircraft and Cruise Missiles

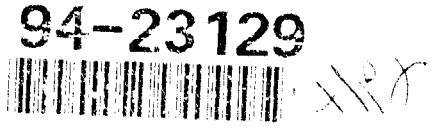
Implications for the Intelligence Community

Myron Hura, Gary McLeod



Project AIR FORCE





The research reported here was sponsored by the United States Air Force under Contract F49620-91-C-0003. Further information may be obtained from the Strategic Planning Division, Directorate of Plans, Hq USAF.

Library of Congress Cataloging in Publication Data

Hura, Myron, 1943–
Route planning issues for low observable aircraft and cruise missiles : implications for the intelligence community / Myron Hura, Gary McLeod.
p. cm.
Prepared for the United States Air Force.
"MR-187-AF."
Includes bibliographical references.
ISBN 0-8330-1368-8
1. Cruise missiles—Guidance systems. 2. Stealth aircraft. 3. Navigation (Aeronautics) I. McLeod, Gary, 1948– II. United States. Air Force. III. Title.
UG1312.C7H87 1993
623.4'519—dc20 93-7687
CIP

Published 1993 by RAND
1700 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
To obtain information about RAND studies or to order documents, call Distribution Services, (310) 393-0411, extension 6686

RAND

Route Planning Issues for Low Observable Aircraft and Cruise Missiles

Implications for the Intelligence Community

Myron Hura, Gary McLeod

Prepared for the
United States Air Force

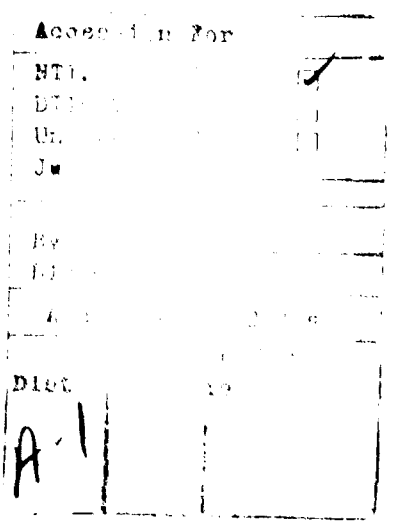
Project AIR FORCE

Preface

This report highlights key issues pertaining to threat penetration analysis and route planning for low observable (LO) aircraft and cruise missiles. It then suggests initial steps to address them. The objective is to assist the intelligence and mission planning communities, the developers of LO weapon systems, and the weapon operators in gaining a better understanding of these issues. Without this understanding, the intelligence infrastructure necessary to support more effectively the employment of such weapon systems in a wide range of threat environments may not be developed.

This report should be of particular interest to Air Force Intelligence Counterpart Officers (ICOs) in assessing threat data and penetration analysis requirements with developers and operators early in the acquisition cycle of LO weapon systems. It also should be of interest to Intelligence Support Working Groups (ISWGs) responsible for developing Intelligence Support Plans (ISPs) for the acquisition of specific LO aircraft and cruise missiles.

The issues discussed in this report emerged from our ongoing work in support of the development of Intelligence Support Plans for designated weapon acquisition programs. That work is sponsored by the Air Force Assistant Chief of Staff for Intelligence (AF/IN) and performed within the Aerospace Technology Program of Project AIR FORCE, a federally funded research and development center at RAND.



Contents

Figures

Summary

Low observable (LO) aircraft and cruise missiles give U.S. military forces the technical capability to successfully attack well-defended ground targets with substantially reduced risk of engagement by enemy defenses. But fully exploiting these new technical capabilities in a range of warfighting scenarios requires developing an intelligence infrastructure that can support the special capabilities and requirements of LO technologies. If this infrastructure is not developed (by upgrading the existing infrastructure), the operational value of LO aircraft and cruise missiles will be sharply reduced.

The intelligence community is responsible for providing a large share of this infrastructure. Developing such support for a new technology is a difficult task made even more challenging by today's budgetary constraints and personnel reductions. Our ongoing work in supporting the Air Force as it develops Intelligence Support Plans for designated weapon acquisition programs has convinced us that the intelligence community should continue to be pro-active in resolving the issues highlighted in this report, otherwise, limited resources will make it extremely difficult for that community to effectively support LO systems.

It is especially important that the intelligence community attain a thorough understanding of two broad areas that are largely the province of those who develop and operate the new weapons systems: (1) the techniques now being developed for threat analysis, penetration analysis, and route selection for LO aircraft and cruise missiles, and (2) potential applications of LO aircraft and cruise missiles, i.e., their concept of operations. To ensure that LO weapon systems are properly supported when they emerge in the operational environment, the ongoing dialogues between the intelligence and mission planning communities, the developers, and the operators should be expanded to include the issues highlighted in this report.

At a minimum, the dialogues between the communities should be expanded to address issues in the following areas:

- Threat data requirements to support LO platform development, testing, and employment
- Characteristics of threat data currently available to support operations
- Constraints on data security and access and potential solutions

- Lack of a plan to validate threat models used in penetration analysis
- Interface requirements of unit-level intelligence support workstations and mission planning systems (e.g., Sentinel Byte/Air Force Mission Support System interface)
- Development of route planning procedures that take into consideration, in a timely manner, mobile threats, airborne interceptors, and anti-aircraft artillery
- Assessment of operational alternatives and methods for operational planning to enhance threat penetration capabilities of LO platforms
- Need for and uses of automated procedures in route planning
- Need for adaptive route planning capabilities onboard aircraft.

Although this list should not be considered all-inclusive, it does identify issues of major concern in developing the intelligence infrastructure to support LO aircraft and cruise missiles. Applicable lessons learned from the employment of LO platforms during Operations Desert Shield/Desert Storm should also be considered in developing an intelligence infrastructure to support other LO aircraft and cruise missiles.

The first two issues are closely coupled and stem from the practice of providing very accurate, tailored threat data to developers for the development and testing of their systems. Typically, such data, except for strategic fixed defense sites, are not available in operational environments. Relying on tailored data, developers may build detailed threat penetration analysis and route selection tools that cannot be adequately supported by operational intelligence threat data. The intelligence community could reduce the likelihood of this problem by educating developers and operators about the types of threat data it can actually provide while coping with all the other demands on national and theater intelligence systems.

Threat penetration analysis models for LO platforms are typically developed under special access programs, with limited visibility to the intelligence community. Similarly, the most accurate and complete threat data are typically classified at security levels for which very few developers are cleared. Development of inadequate threat penetration analysis models for LO aircraft and cruise missiles may result from the limited access of the intelligence community to LO performance data on the one hand, and that of developers to threat data on the other hand.

Similar data-access constraints affect the quality of threat penetration analysis and route selection of LO platforms in the operational environment. The best

threat data should be provided to operations intelligence personnel and aircrews for planning LO platform routes. And the most current and accurate LO performance data should be used in threat penetration analysis.

Because of the complexity involved in creating threat models and the cost and time required to validate them, the Department of Defense typically does not furnish validated threat models to developers. Thus, LO aircraft and cruise missile developers often construct their own threat models or modify unvalidated models to test their systems; or they fund equipment contractors to do it for them. These models may inaccurately reflect threat capabilities. Also, to minimize computing requirements and associated costs, developers may aggregate threat data to such an extent that required resolution is lost. To alleviate these and other potential problems, the intelligence community, in coordination with the mission planning and system acquisition communities, should, at a minimum, define the level of detail and the spectrum of generic threats and threat characteristics that developers must consider in developing threat penetration models.

Developers of unit-level intelligence support systems may not have visibility into the threat analysis and penetration models of mission planning systems for LO platforms. Without a good understanding of the type of threat data required by LO platforms, and how that data will be used in route planning, developers of unit-level intelligence support systems may be building databases or files that are of limited value. Moreover, they may develop threat-data update protocols and procedures that may preclude responsive support for mission planning systems. Intelligence Support Working Groups are good forums for addressing such issues.

Typically, aircraft mission planning systems do not include mobile threats, airborne interceptors, and anti-aircraft artillery in their threat penetration analysis. The dynamic nature of mobile and airborne interceptor threats requires the development of probabilistic threat laydowns, a capability that has not been built into existing aircraft mission planning systems. Similarly, aircraft and cruise missile mission planning systems, in selecting preferred routes against heavily defended targets, do not include provisions for incorporating tactical alternatives, such as defense-suppression missions, deception, countermeasures by other platforms, and other operational tactics. To determine to what extent these shortcomings can be corrected in future threat penetration analysis models of mission planning systems for LO aircraft, and because a wide range of operational options may not be easily incorporated into automated mission planning systems, an assessment should be conducted to examine the proper role

of such systems and the level of detail that should be included in them to aid operational mission planners.

Adaptive route planning (receiving and analyzing near-real-time threat data and modifying a route while en route to the target) may be an important capability for enhancing the survivability of LO aircraft. Information collected from onboard and offboard sensors or from the last raid will be particularly important to LO aircraft penetrating high, overlapping threat environments. Adaptive route planning is a relatively new concept; however, without stated requirements and support, it is unlikely to be developed. Operators (in coordination with the intelligence community) and developers should determine whether such a capability is required and, if required, formulate a development plan. In formulating the plan, they will need to consider how to deal with the complexity of deconfliction, timing, and reallocation of other assets when aircraft with adaptive route planning capabilities change routes.

Expanded dialogues between decision makers are the necessary first step in resolving the issues highlighted in this report. With a good understanding of these issues, more effective working relationships can be established between the developers, the intelligence and mission planning communities, and the operators of LO aircraft and cruise missiles. The improved working relationships should assist the Air Force intelligence community in setting priorities and in allocating resources to develop the intelligence infrastructure necessary to support more effectively the employment of LO aircraft and cruise missiles.

Acknowledgments

The work presented in this report benefited from the reviews and comments of several individuals. In particular, we would like to thank Maj Robert Butler (HQ AF/INXA) and Maj Robert Heston (HQ AF/INXX) from Headquarters, Air Force, and LtCol William Craig (HQ ACC/DRIC) and LtCol Eugene Schempp (HQ ACC/DRX) from Headquarters, Air Combat Command, for their comments and suggestions on an earlier draft of this report. We are also indebted to our RAND colleagues Bart Bennett and David Frelinger for their useful insights and suggestions.

Acronyms and Abbreviations

AAA	Anti-aircraft artillery
ACM	Advanced Cruise Missile
AFMSS	Air Force Mission Support System
AFOTEC	Air Force Operational Test and Evaluation Center
ALCM	Air-Launched Cruise Missile
ATO	Air Tasking Order
DT&E	Developmental test and evaluation
DTED	Digital Terrain Elevation Data
EOB	Electronic order of battle
GPS	Global Positioning System
HUMINT	Human intelligence
ICO	Intelligence Counterpart Officer
IDB	Integrated Data Base
IOC	Initial operational capability
ISP	Intelligence Support Plan
ISWG	Intelligence Support Working Group
LO	Low observable
MIIDS	Military Integrated Intelligence Data System
MSS	Mission Support System
NRT	Near-real-time
OT&E	Operational test and evaluation
RCS	Radar cross section
RWR	Radar warning receiver
SAM	Surface-to-air missile
SAR	Special access required

SB	Sentinel Byte
SCI	Sensitive compartmented information
SEAD	Suppression of enemy air defenses
STAR	System Threat Assessment Report
TAMPS	Tactical Aircraft Mission Planning System (Navy)
TEMP	Test and Evaluation Master Plan
TENCAP	Tactical Exploitation of National Capability
TLAM	Tomahawk Land Attack Missile (Navy)
TMPC	Theater Mission Planning Center
TMPS	Theater Mission Planning System
XIDB	Extended Integrated Data Base

1. Introduction

The development of low observable (LO) technologies and their application to several combat aircraft and cruise missiles provide U.S. military forces with the technical capability to successfully penetrate and transit enemy air space, then attack well-defended ground targets with substantially reduced risk of engagement by enemy defenses. Adequate threat data, threat penetration models, and route planning procedures are required to fully exploit the technical capabilities of these LO weapon systems in a range of warfighting scenarios.

The intelligence community is responsible for providing a large share of this support. To do so effectively, it must attain a good understanding of both the techniques for threat penetration analysis and route selection being developed for LO aircraft and cruise missiles and their potential applications, i.e., their concept of operations. Similarly, LO weapon developers and operators need to understand the current capabilities and potential limitations of the intelligence community in providing such required support as a description of a threat's capabilities (detection, tracking, and engagement), its location, and its current status.

Therefore, effective dialogues between the intelligence and mission planning communities, the developers of LO weapon systems, and the operators are essential to ensure that these systems are properly supported when they emerge from the developmental environment into the operational one. As an aid to these dialogues, this report discusses threat penetration analysis and route planning for LO aircraft and cruise missiles and highlights key issues that need to be addressed and resolved.

Role of Mission Planning

In discussing these issues, we use conventional mission planning systems as a focal point. A primary function of such systems is to help aircrews and/or cruise missile planners select routes with the lowest risk of attrition to enemy defenses. Therefore, mission planning systems highlight the areas where operators, system developers, and the intelligence and mission planning communities most need to expand their dialogues (informal, as well as formal, working relationships and exchanges of information). The remainder of this section describes mission planning systems and includes special considerations for LO technologies.

Typically, aircrews and cruise missile planners develop low-risk routes using the threat penetration models of mission planning systems. Such systems rely on threat data provided by the intelligence community. For example, the Air Force mission planning system, Mission Support System II (MSS II), and its follow-on, Air Force Mission Support System (AFMSS), receive threat data from Sentinel Byte (Ref. 1), a unit-level intelligence workstation, to create a threat laydown. The threat laydown is then superimposed on Digital Terrain Elevation Data (DTED), a terrain database produced by the Defense Mapping Agency. The resulting threat space takes into consideration the effect of terrain masking. It is used to select preferred mission routes that minimize aircraft exposure to enemy defenses.

On current conventional aircraft mission planning systems, such as the Air Force MSS II and the Navy Tactical Aircraft Mission Planning System (TAMPS) (Ref. 2, Section 7.0), aircrew members manually enter route waypoints on electronic displays. Aircraft-specific algorithms then determine whether the selected routes can be flown, taking into consideration aircraft aerodynamic characteristics, aircraft weight (including fuel and weapon payload), and environmental conditions, e.g., winds, temperature, and humidity.

Future upgrades of AFMSS are projected to have autorouting capabilities designed to more rapidly and, presumably, more accurately select low-risk routes based on presented threats. The Air Force has not yet selected the autorouting concept for AFMSS. At least two generic autorouting concepts are being considered.

The first autorouting concept has three elements: (1) an aircraft or cruise missile performance model, (2) an algorithm that adds the numerical value assigned to each cell of the threat space through which the aircraft or cruise missile can pass, then selects the route with the lowest cumulative value, and (3) associated databases. The concept requires the precalculation of a threat space. This process is time consuming if a low-speed processor is used to develop a threat space for a large area: Not only must a large number of threats be assessed, but the DTED for this large area is usually reformatted. This concept is not responsive to threat updates.

The second autorouting concept includes the following three elements: (1) an aircraft or cruise missile performance model, (2) a database of precalculated threat templates for selected aircraft headings and altitudes, and (3) an algorithm that, in real-time, places threats at a specific location, pulls the appropriate threat template from the database, and routes the platform while minimizing its exposure to the threats. This concept does not require the preprocessing of a

threat space and, therefore, can be more responsive to threat updates. However, it treats threats in a more aggregated and simplified manner than the first concept.

Whether a manual or automated route selection technique is applied, an understanding of the quality and currency of the threat data, as well as the quality and validity of threat penetration analysis and modeling, is essential.

The route planning process for the Navy Tomahawk Land Attack Missile (TLAM) is substantially different from that for aircraft armed with conventional weapons. Mission planners for Tomahawk select routes on the basis of results from simulations on the Theater Mission Planning System (TMPS) at the Theater Mission Planning Center (TMPC) (Ref. 3). This procedure uses a missile model to fly through the threat space a statistically significant number of times. It takes into account missile navigation errors and determines the probability of survival for the particular mission route. Similar procedures are employed in planning routes for Air Force cruise missiles: the Air-Launched Cruise Missile (ALCM) and the Advanced Cruise Missile (ACM). Despite the substantial differences in route planning procedures between cruise missiles (TLAM, ALCM, and ACM) and aircraft, most of the threat penetration analysis and route planning issues discussed in this report are applicable to both LO aircraft and cruise missiles. We note that the B-2 autorouter can be used to select routes for ACMs.

Report Scope and Organization

This report addresses generic LO manned aircraft; however, the focus is on bombers and ground-attack fighters for which threat avoidance is high priority. For other types of LO aircraft (such as air-superiority fighters) that are engaged in offensive operations but have missions other than air-to-ground weapon delivery, threat avoidance may be of lower priority.

Although both LO aircraft and cruise missiles are discussed, the survivability of individual, conventionally armed cruise missiles is relatively less important than that of individual aircraft. Cruise missiles are not manned and are much less expensive; offsetting the lower cost of the cruise missile is its inability to react to defenses. Aircraft can, in some situations, if necessary, manage with fewer data because of their greater ability to react to threats. (However, when aircraft deviate from the preplanned route, they no longer are on the "optimal" route for survivability; also, they may conflict with other assets of a raid group or may limit the effects of supporting assets from that point on.) Thus, the accuracy of

threat data and the fidelity of the threat penetration models required for route planning may be different for aircraft and cruise missiles.

This report is organized as follows. We first describe threat penetration analysis and route planning objectives and procedures for LO aircraft and cruise missiles during development and testing in Section 2. Then, we describe threat analysis and route planning in an operational environment in Section 3. Finally, we discuss important implications for the intelligence community in providing threat data and analytical support for operational mission planning systems in Section 4.

2. Threat Penetration Analysis and Route Planning During Development and Testing

The primary advantage of LO aircraft and cruise missiles is their low radar cross section (RCS). A low RCS substantially decreases susceptibility to detection by early-warning radars and acquisition radars, thereby delaying or eliminating the subsequent handoff to the fire control radars of surface-to-air missile (SAM) systems or airborne interceptors. A low RCS also complicates the problems of missile tracking and warhead fuzing in the event that a SAM or an air-to-air missile is launched. Properly managed, a low RCS can markedly reduce the risk of successful engagement by enemy defenses and thus increase aircraft and cruise missile survivability.

LO aircraft also may be equipped with active and passive countermeasures, and possibly organic defense-suppression weapons to further increase penetration capabilities. The expense may not be warranted to develop these capabilities for cruise missiles.

Typically, system specifications for LO platforms require meeting specific RCS levels and may require a particular measure of survivability or probability of arrival at the target or weapon launch basket. System specifications for aircraft may also require the development of a measure of survivability for a full mission, both ingress and egress. Thus, the primary objective of threat penetration analysis and route planning during developmental test and evaluation (DT&E) is to demonstrate the capability of meeting contract systems specifications.

During operational test and evaluation (OT&E), the developed penetration analysis, route planning procedure, and LO platform are tested as a system to determine their capability of meeting operational requirements, which may include criteria not listed in contract system specifications. And, if aircraft are equipped with other penetration aids or self-defense systems, tests are also conducted to ascertain whether these systems meet operational requirements.

This section discusses some of the issues pertaining to threat penetration analysis and route planning that can arise during development and testing of LO aircraft and cruise missiles.

LO Platform Characteristics

In the development and test phases of LO aircraft and cruise missiles, extensive RCS analysis and measurements are conducted, at various aspect angles and at various frequencies, and the results are recorded. Those data are then formatted into matrices for threat penetration analyses that examine aircraft or cruise missile survivability. After validation, the RCS data collected during the development and test phases are typically entered into databases for use by the mission planning system.

Provisions to modify the mission planning databases to reflect RCS changes of LO aircraft (usually increases) caused by maintenance actions or operational employment may or may not be part of the development program. Operators of LO aircraft will want this RCS-management capability.

The information collected during the test phase about the performance of other penetration aids and self-defense systems on LO aircraft also may not be translated into models and databases for hosting on mission planning systems. Typically, this type of information is used only in developing algorithms and procedures that are incorporated into training systems and taught to operators. **Therefore, LO aircraft developers may not provide threat penetration models (for hosting on mission planning systems) that have the capability of examining the synergistic effects of RCS management and other penetration aids on route selection.**

Threat Penetration Analysis and Route Planning

In parallel with or after developing appropriate threat penetration analysis models, developers of LO aircraft and cruise missiles must demonstrate the capabilities of these platforms to penetrate simulated real-world defenses. To demonstrate these capabilities, developers will most likely generate preferred routes, using their threat analysis models and route selection algorithms. Then, independent testing organizations will probably run the routes through other threat penetration models and determine the survivability of the platforms on the preferred routes.

A notional threat penetration model consists of various threat models overlayed on a terrain model (digital maps or DTED), a terrain-masking algorithm, and a model of aircraft or cruise missile characteristics with associated RCS data.

Such threat penetration models may, at one extreme, be full simulations in which aircraft or cruise missiles are "flown" against the threats with simulated

detection, acquisition, handoff to fire control systems, weapon launch and fly-out, and fuzing and warhead fragmentation patterns. Based on these simulations, the probability of aircraft or cruise missile survival is calculated for each route flown. Obviously, this category of penetration analysis requires substantial computer resources (including a comprehensive, and often detailed, database) and can take considerable time (several hours to a few days) to perform.

At the other extreme, such models may consist simply of a threat space, with a single lethality number or attribute for an aircraft or cruise missile entering a specific cell of the threat space, and an algorithm for calculating an overall survivability score for an aircraft or cruise missile along a particular route to the target. The single lethality number for each cell of the threat space is precalculated using appropriate threat locations and postulated capabilities; it would also take into account terrain obscuration (simple line-of-sight calculations) and the characteristics of the LO platform.

LO aircraft and cruise missile developers are typically under contract to develop route planning tools for mission planning systems. They may use one of the preceding categories of threat penetration models or an intermediate variation. The integration of these tools on existing or planned mission planning systems may or may not be the responsibility of the aircraft or cruise missile developer. **If platform developers are not responsible for the integration, close coordination must be established between them, the intelligence community, and mission planning system developers to ensure that the threat penetration model is properly integrated and that the data required to support the model in an operational environment are available.**

Threats Considered in Developing Penetration Models

Design specifications for LO platforms may not call for the development or use of threat analysis and penetration models that consider all generic categories of threats, e.g., early-warning radars, radar-guided and infrared-guided SAM systems, anti-aircraft artillery (AAA), airborne interceptors (possibly with infrared search and track systems), and jamming threats to Global Positioning System (GPS) receivers. Sea-based threats, particularly ship early-warning and surveillance radars, are often overlooked.

Therefore, early in the LO platform's development, it is important to determine specifically which threats will be considered; this information should be contained in the System Threat Assessment Report (STAR) specifically tailored

for the LO platform (Ref. 4, Part 4, Section A). Typically, the models developed for export to mission planning systems focus on ground-based radar threats, particularly SAM systems. Often, they do not include either radar or optically directed AAA, or infrared-guided SAM threats. They may include air surveillance platforms, but typically do not include airborne interceptors.

Decisions for not including AAA and airborne interceptors in threat models of mission planning systems need to be reevaluated. The capabilities of an individual AAA system against aircraft and cruise missiles are small. However, several AAA systems, clustered together and properly alerted, pose a measurable threat to aircraft or cruise missiles flying at low altitudes. Also, airborne interceptors in the vicinity of the target area, or along the routes of LO aircraft, can create a substantial threat. They pose some risk to LO cruise missiles if they are positioned very close to the missile routes.

In reevaluating the need for incorporating AAA and airborne interceptors in threat models, decisionmakers must weigh the benefits of doing so against two significant difficulties:

- Because the threat footprint of airborne interceptors is large and can change rapidly over time, threat penetration models would be complex and time-consuming to run.
- It might not be possible to establish and maintain current locations for either AAA or airborne interceptors over the course of the mission planning and execution cycle.

To some extent, the above concerns also apply to early-warning radars and SAM systems as these systems become more mobile.

If the models do not take into consideration AAA or airborne interceptors, operations intelligence personnel, mission planners, and aircrews will be forced to increase their work load measurably to deal manually with such threats, on a case-by-case basis. For example, in an airborne interceptor threat environment, they will have to manually determine whether air superiority is essential before committing LO aircraft. Or, in dense SAM and AAA environments, they will have to establish the relative values of flying above AAA engagement envelopes while increasing the aircraft's susceptibility to SAM systems, or flying low to minimize susceptibility to SAM systems while increasing the exposure to AAA. These decisions may well be based on concepts of operations, tactical intelligence, or combat conditions that are difficult to automate.

This discussion is not meant to argue for or against including AAA and airborne interceptors in threat penetration models, but to highlight the issues, and, more important, to emphasize the need for timely information on these generic threats within the theater of operations.

Platforms that use GPS data to update their inertial navigation systems while en route to target areas may also be vulnerable to GPS jamming threats. Given the location of GPS jammers, mission planners of such platforms may be able to select highly survivable routes while maximizing the probability of GPS acquisition. Data on GPS jammers are particularly critical to autonomous cruise missiles that rely solely on GPS-aided inertial guidance to strike their targets. Procedures must be established to ensure that operations intelligence personnel and mission planners can obtain timely data on GPS threats for their areas of interest.

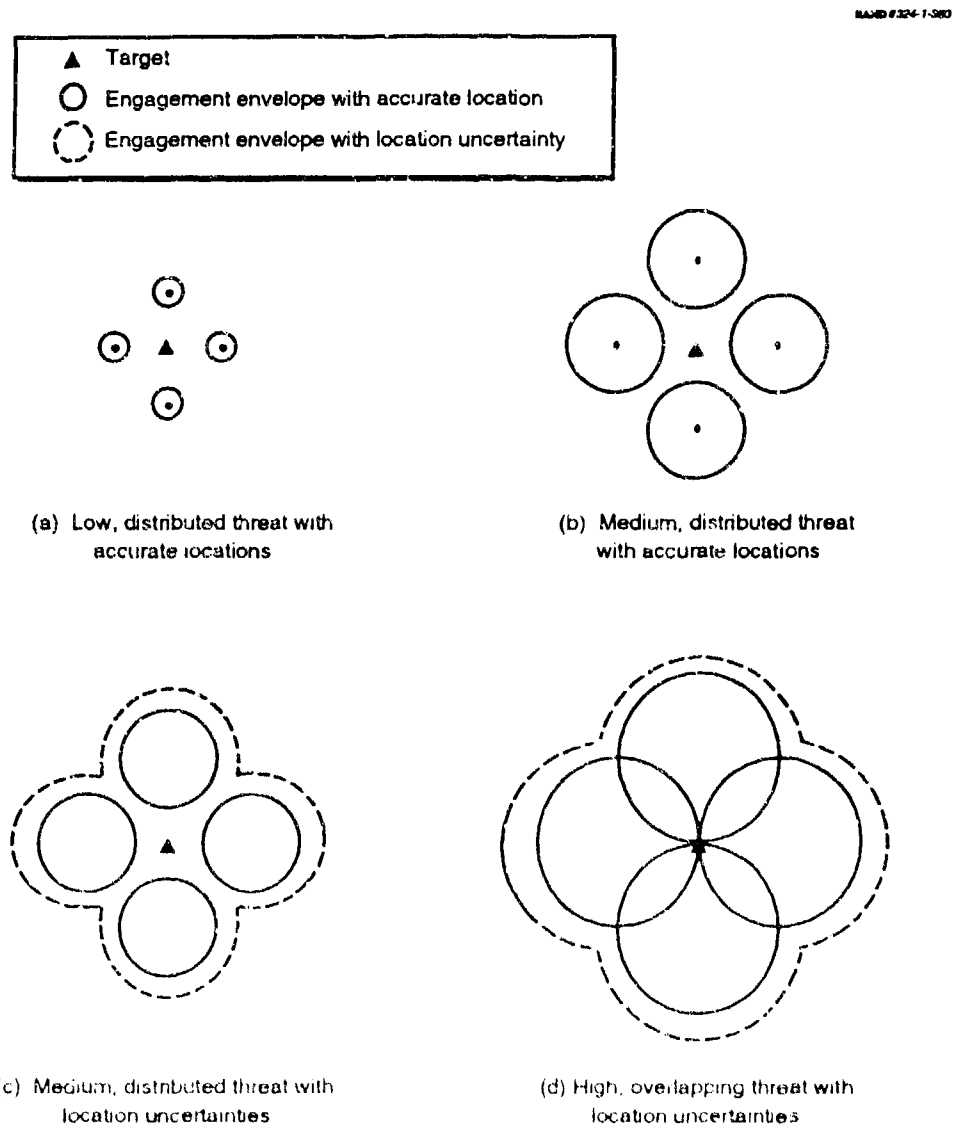
Threat Data and Threat Environments

In assessing the threat penetration capabilities of LO platforms and the subsequent development of appropriate threat penetration models, developers rely on government-furnished threat data and approved threat environments. **The threat data provided may not be representative of the threat data available in an operational environment, and they may not correspond exactly to the input parameters of the penetration model.** For example, precise locations of air defense systems are provided. In an operational environment, however, the threat location accuracies will vary according to the source of data: locations derived from survey data or geocoded imagery (usually stereo) are the most precise. Adequate provision must be made for including location uncertainty in threat penetration models of autorouters; otherwise, the results derived from their use in an operational environment may be suspect.

Threat location inaccuracies are particularly critical for route selection techniques that consider terrain masking. For example, the placement of an early-warning radar on a mountain top will yield substantially different line-of-sight calculations than if the radar is placed at the base of the mountain. Thus, these inaccuracies may lead to the selection of improperly assessed routes.

Threat environments provided to LO platform developers may substantially influence developers' designs of route planning procedures or algorithms. To illustrate this issue, we postulate four notional threat environments, with threat capability, density, and location uncertainties as parameters (see Figure 1):

- A low, distributed threat with accurate threat locations (Figure 1a)
- A medium, distributed threat with accurate threat locations (Figure 1b)
- A medium, distributed threat with uncertainties about threat locations (Figure 1c)
- A high, overlapping threat with uncertainties about threat locations (Figure 1d).



NOTE: For simplicity, threat envelopes are shown as two dimensional and circular; in reality, for both LO and non-LO platforms, they are three-dimensional volumes with complex structure.

Figure 1—Notional Threat Environments

The designs would be affected as follows. In a low, distributed threat environment with accurate threat locations, LO aircraft and cruise missiles can easily avoid the small number of low-capability threats. In a medium, distributed threat environment, again with accurate threat locations, LO platforms are also likely to avoid defenses. For both environments, a rudimentary autorouter or a manual procedure could be used in selecting routes to avoid defenses. Under these conditions, the advantage of the rudimentary autorouter over a manual procedure would be in decreasing route planning time, from hours to minutes. This advantage may be crucial because it enables responsive route planning for a large number of missions.

A medium, distributed threat environment with uncertainties about threat locations poses somewhat different challenges to route planners. In this environment, the specific location of the threat is unknown; the threat could be located within an uncertainty basket of several miles. Such uncertainty results in probabilistic engagement envelopes that overlap, thereby precluding free access to the target. Under these conditions, neither a rudimentary autorouter nor a manual procedure can select a route that avoids all defenses. Instead, a sophisticated autorouter that can simulate aircraft or missile flight over a probabilistic threat space might be useful in determining preferred routes. For an LO aircraft, the preferred route would be the route with the lowest calculated risk factor. As an added precaution, aircrews would be prepared to utilize other means at their disposal to counter those threats, should they materialize. For LO cruise missiles, a sophisticated autorouter again would be used to calculate risks of engagement for a statistically significant number of simulated routes. However, mission planners would then select two or more low-risk routes (rather than one route) to minimize the probability that all missiles attacking a target complex could be engaged by the same defense systems.

In a high, overlapping threat environment, LO platforms are more susceptible to threats, and even very precise route selection procedures or algorithms may not significantly decrease risk of engagement. Under these conditions, the development of additional planning tools that incorporate penetration aids and tactics may be required. Such tools would include a wide range of radar jamming systems, SEAD (suppression of enemy air defenses) aircraft, fighter escorts, and other defense-suppression assets. It is unlikely that autorouters can be built to include all the decision criteria required by such tools, particularly since the criteria will likely develop over time with training and combat experience. This eventuality suggests that the design of autorouters must include adequate provisions for operator interaction in the route selection process.

The notional threat environments do not include all possible combinations of threat densities, threat location uncertainties, or uncertainties about defense engagement envelopes as a function of RCS; nor do they include mobile threats or airborne interceptors. They only highlight issues that should be considered in developing specifications for a common autorouter for LO platforms, and they illustrate conditions that developers of precise autorouters should consider. Perhaps the primary objective of an autorouter should be to substantially decrease the time, and potentially the expertise, required for route planning.

The Air Force is now in the process of examining the concept, need, and feasibility of developing a common autorouter for LO platforms. The process should include an examination of the frequency of threat environments and/or conditions that are likely to be encountered to determine what level of sophistication is appropriate for a common autorouter. We consider this step necessary to ensure that the proper balance is established between demands on intelligence and operational communities to support an autorouter, and demands for other intelligence and mission planning functions to support LO platform employment in the most-likely threat environments.

Operational Evaluation of LO Platforms

Before an LO platform achieves initial operational capability (IOC), it must successfully complete OT&E, conducted by independent service organizations. In the Air Force, OT&E is performed by the Air Force Operational Test and Evaluation Center (AFOTEC). It is at this stage of the system's acquisition process that LO platforms must demonstrate the capability of meeting specified test standards for survivability, under conditions that represent operational environments. In an ideal situation, that capability would consist of four steps: (1) developing survivable routes using the penetration models within the operational mission planning system; (2) flying the routes against real systems, including representative threat location uncertainties and, possibly, uncertainties in threat performance; (3) employing penetration aids, as needed; and (4) evaluating the results against system specifications.

Obviously, the costs of procuring real threat systems and flying a sufficient number of routes, under appropriate security conditions to protect LO characteristics, are prohibitive. At best, LO aircraft and cruise missiles are flown a number of times against a select number of individual, representative sites. For the most part, testing the effectiveness of the mission planning penetration models to develop survivable routes is done with simulations.

The lack of good communications between the developers and operational test personnel can lead to a number of problems. We present several hypothetical problems here.

- Performance models in the simulation may include capabilities that are not included in the mission planning penetration models. For example, the latter may not include all the modes of the threat radar.
- System specifications may not match those in the Test and Evaluation Master Plan (TEMP), or may not be easily translatable. For example, the specifications of cruise missile systems may call for a certain high probability of arrival at the target, assuming a specified number of simulation runs. However, operators may want the probability of arrival calculated for each mission, because they need high confidence that a particular target will be destroyed, not high confidence that many of the intended targets will be destroyed.
- System specifications may call for testing survivability against only certain threats, assuming precise positioning, whereas the simulations may probabilistically position threats to account for threat-data uncertainties.

Data Security

The security classification of pertinent data is a significant difficulty in coordinating the development and testing of threat analysis, penetration analysis, and route planning tools for LO aircraft and cruise missiles. Most LO platform survivability improvements have been developed under special access programs. Consequently, information important to understanding threat data requirements is available only to a very small number of intelligence personnel. Conversely, the most accurate and complete threat data available may be classified at a security level for which developers may not be cleared. Moreover, some threat databases cannot be released to contractors. Thus, while they are developing threat models, penetration models, and route planning techniques, developers may not have visibility into all available threat data.

This problem of limited access to data places a great burden on the few individuals in the intelligence community who are cleared for both LO platform special access required (SAR) data and sensitive compartmented information (SCI) threat data.

- They must understand how threat data are being used in LO platform design and in threat and penetration models, and they must understand how the

accuracy and content of the threat data affect the survivability of the LO platform.

- They must provide sanitized threat data that meet developers' requirements for testing system technical specifications.
- For the operational evaluation phase, they must ensure that the threat data provided are representative of the data that will be available to support real-world operations.

Effective working relationships between developers, intelligence personnel, and operational test personnel with the proper security clearances are essential in minimizing potential problems.

Access restrictions associated with LO aircraft and cruise missile performance data and with SCI threat data also occur in the operational environment. One approach to alleviate this problem is to ensure that the following three criteria are met: (1) operations intelligence personnel and aircrews responsible for route planning of LO platforms have the necessary clearances, (2) they perform intelligence support and mission planning functions in secure facilities, and (3) they employ intelligence support and mission planning systems specifically designed to support LO platforms.

As the number of LO platforms increases, the preceding approach may be impractical for the following reasons: Operations intelligence personnel and aircrews responsible for threat penetration analysis and route planning may not be cleared for SAR and SCI data; a common mission planning system to support both LO and non-LO platforms (the goal of AFMSS) may be developed; and costs may preclude the building of secure facilities.

Perhaps one method of dealing with these problems will be to build separate databases and application software that are not directly accessible or cannot be read, displayed, or copied (this assumes, of course, that software can be written to provide the necessary security control). For example, the platform RCS database may be accessible only through an executive program that reads applicable portions of the database and directly inputs the specific data into the application software for building threat spaces. Obviously, the success of this approach will depend, for the most part, on the confidence that personnel responsible for route planning have in the generated results.

3. Threat Penetration Analysis and Route Planning in an Operational Environment

The preceding section discussed some of the issues pertaining to threat penetration analysis and route planning that can arise during development and testing of LO platforms if effective working relationships are not established and maintained between the developers of LO aircraft and cruise missiles, the intelligence and mission planning communities, and the operators. The extent to which these issues matter is a function of operational considerations. Moreover, operational considerations shape the solutions that should be pursued in developing threat penetration models for mission planning systems to support LO platform employment.

The important difference between threat penetration analysis and route planning during the development and testing of LO platforms and threat analysis and route planning for real-world operations is that, whereas the primary objective of such analysis and planning during development and testing is to ensure that LO system specifications and projected operational requirements are met by contractors, the primary objective of such analysis and planning for real-world operations is to assist aircrews and mission planners to meet warfighting objectives, taking into consideration LO platform capabilities to enhance survivability.

Operators are interested in route planning tools that consider accuracy, completeness, timeliness of operational intelligence data, and speed of routing, as well as all options for enhancing aircraft survivability. They are not interested in route planning tools that could be very precisely solving the wrong problem and, worse, providing a false sense of security.

This section discusses some of the issues that we consider important in developing operationally useful threat penetration analysis and route planning tools for LO aircraft and cruise missiles.

Location, Accuracy, and Completeness of Threat Data

In planning operational missions, aircrews and mission planners rely on threat data provided by the operations intelligence community. The location accuracy

of the data will vary according to the category of defense systems and the sources used in collecting the data.

The most accurate and complete threat data are those on fixed and mobile defense systems employed to protect well-known strategic target areas. Those data contain precise geodetic locations of individual emitters and list accurately all operating parameters. Such data are collected over long times by a combination of national and theater sensors and are analyzed by centralized intelligence activities. However, the data may not be current or complete enough, and thus may have only a limited value in route planning of LO platforms.

More current, and usually less accurate, information on active threat emitters is collected by theater and tactical sensors. For example, this category of information may be available to operators in near-real-time (NRT) from platforms such as Rivet Joint, via broadcast systems such as Constant Source.

Thus, operations intelligence personnel and mission planning personnel are confronted with the problem of correlating threat information of different content and accuracy. If they do not properly correlate and fuse threat data from alternate sources, purge duplicate reports, and delete outdated information, the number of apparent threats may proliferate to the point that the threat files passed to mission planning systems become unusable—a particularly critical issue for mobile threats.

How well operations intelligence personnel and mission planning personnel correlate threat data may significantly affect route selection procedures, particularly if all emitters are not active in high, overlapping threat environments. Under these conditions, threat locations, in particular, should be treated probabilistically (using uncertainty radii), and route selection should reflect these considerations. Also, operations intelligence personnel should be able to appropriately fill in missing threat characteristics needed to support threat penetration analysis or, if unable to do so, should inform the operators of the possible effects on route planning analysis.

In addition to threat location and characteristics data, operators need to know how operationally effective the enemy defenses are relative to their technical capabilities (typically, only technical capabilities are reflected in threat analysis and penetration models of mission planning systems). For example, answers to the following questions can be crucial in selecting ingress and egress routes in a high, overlapping threat environment.

- Are the personnel manning the air defense systems well trained?
- Are the systems properly maintained?
- Are individual systems well integrated?
- Does their doctrine or tactics limit them operationally?

Human intelligence (HUMINT) is probably the best source for this category of data. Increased emphasis on integrating archival and current threat data into mission planning for operations within heavy threat environments may be warranted.

The importance of NRT, electronic order of battle (EOB) data and air defense operational effectiveness data in the notional high, overlapping threat environment, is illustrated in Figure 2.

Without such data, aircrews would be unable to select a low-risk route. Assuming that NRT data indicate that defense systems in one quadrant are inactive, and HUMINT data indicate that maintenance of these systems is typically poor, a low-risk route can be selected with high confidence. Obviously, if only NRT data were available, aircrews could still select a low-risk route, but with less confidence.

In some high, overlapping threat environments, the effects of background clutter and propagation phenomena (such as multipath and ducting) on the performance of acquisition radars may also be important in route planning low-altitude, terrain-following LO platforms. For example, without taking into consideration background clutter, the threat penetration analysis for a well-defended target, located in a narrow valley, may show that there are no low-risk routes into the target. If the background clutter of the high mountains on one side of the valley is taken into consideration, a low-risk route might be found.

Obviously, to determine the effects of background clutter and propagation phenomena on route planning, operators must be provided with the necessary data, to create clutter and reflectivity maps, and with the appropriate threat penetration models. However, because of difficulties in creating high-fidelity clutter and reflectivity maps, variabilities in background clutter and reflectivity (generic models may not suffice), time constraints (extensive computations are required), and the desire to be offense conservative, most route planning procedures assume no background clutter or propagation effects on enemy defenses. Nevertheless, as we have discussed above, developing the capability to account for these effects in route planning of LO platforms may be warranted.

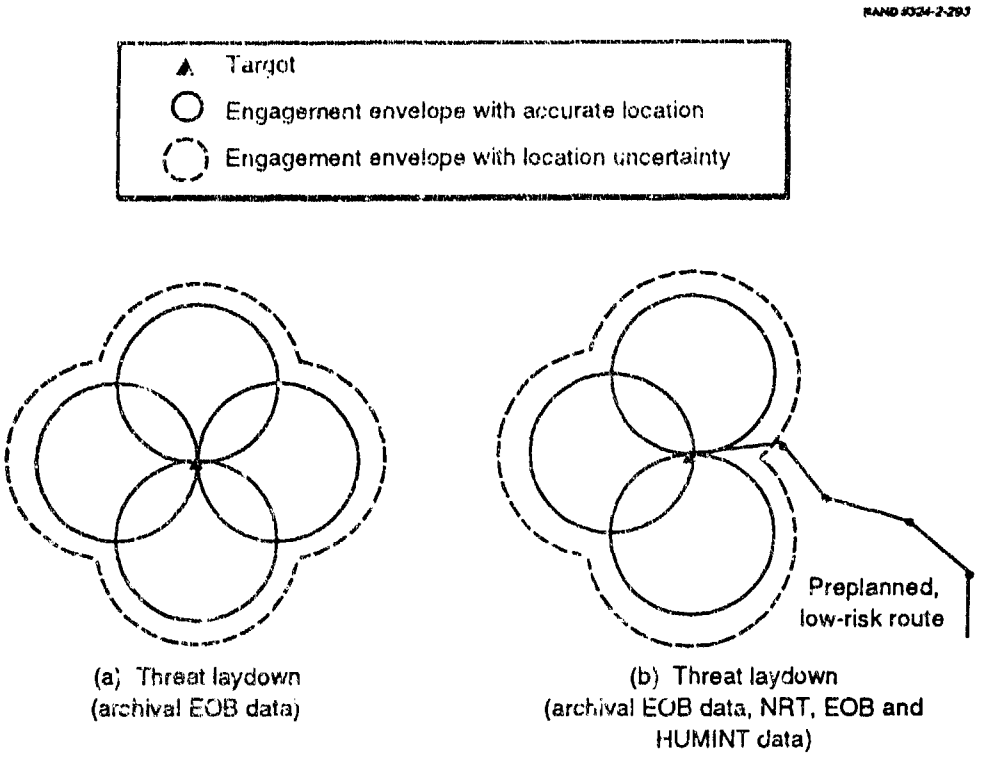


Figure 2—Importance of NRT, EOB Data and Air Defense Effectiveness Data

Timeliness

In planning missions, aircrews and cruise missile mission planners also must consider the time element. They may have to be responsive to abbreviated Air Tasking Order (ATO) cycles (hours rather than one to three days). In very short ATO cycles, it may not be possible to perform time-intensive threat data validation, high-fidelity simulation, and time-intensive route selection procedures. Existing automated manufacturing systems, designed to produce answers rapidly and then adaptively improve the quality of the answer as time is available, should be examined for applicability to responsive route planning. Unless responsiveness measures are included in system specifications, developers of LO aircraft and cruise missiles may not develop rapid threat analysis models and route selection tools for incorporation into mission planning systems.

Alternatively, aircrews and cruise missile planners may have to respond rapidly to emerging tasking for which there are no prebuilt terrain and/or threat spaces.

In this class of contingency, the start-up time for route planning may be most important. With data available, the creation of threat and terrain spaces for large areas of responsibility may require substantial computer processing capabilities. If developers are not required to meet specific start-up-time objectives, they may develop rudimentary applications software and techniques, or perhaps select less capable computers to reduce cost, without considering important operational concerns.

Operational Alternatives to Enhance LO Penetration Capabilities

On the positive side, the planning of real-world operations of LO platforms will typically consider a broader range of methods for accomplishing missions than those produced and evaluated by developers. These methods may include use of the following capabilities:

- Onboard countermeasures
- Multiple similar systems, e.g., lead and wingman cooperation or coordinated cruise missile strikes
- Support assets, e.g., Wild Weasel and EF-111
- Platform employment options.

For example, if threat penetration analyses for LO aircraft, using solely RCS management, result in routes with unacceptable probabilities of attrition, mission planners may call for coordinated defense suppression by supporting aircraft. Under the same conditions, cruise missile planners may call for coordinated cruise missile strikes to saturate (or attack) defenses to ensure that a sufficient number of follow-on missiles arrive at the target. In this example, the tactics are different because the survivability of individual cruise missiles is assumed to be less important than that of aircraft.

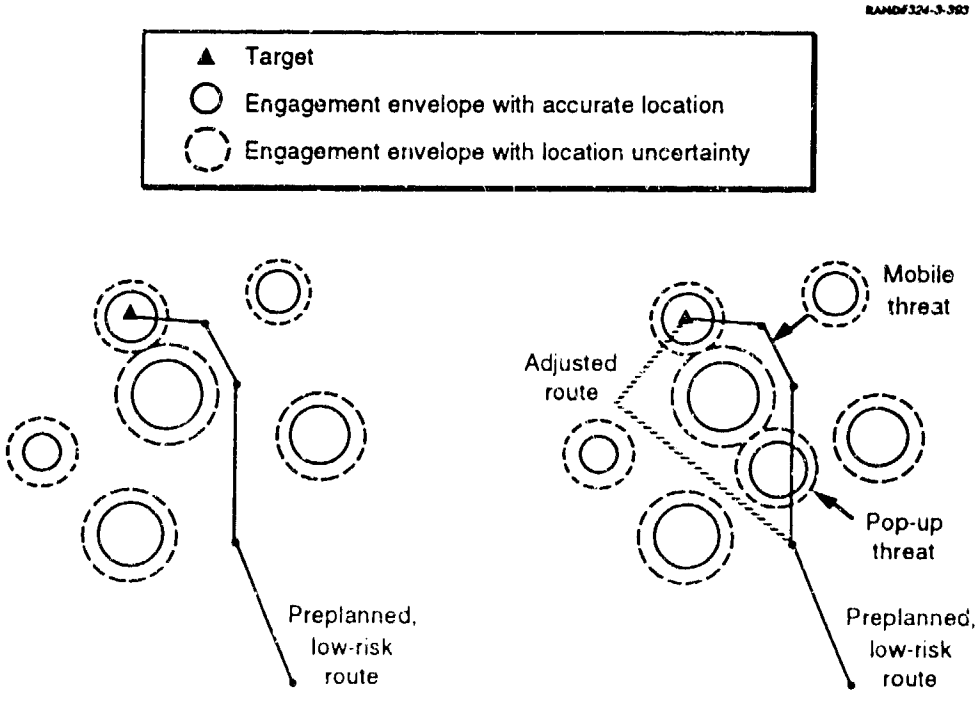
Alternatively, mission planners may have the option of employing standoff jammers, launching decoys, and conducting deceptive maneuvers to diminish capabilities of enemy defenses. These tactical options can be employed individually or in combinations. A route selection technique that accurately takes into consideration these diverse alternatives, as well as the RCS of the LO platform, is likely to be of high interest to operators.

Adaptive Route Planning

Adaptive route planning may be an important capability for enhancing the survivability of LO aircraft. Adaptive route planning consists of receiving and analyzing NRT threat data while en route to the target so that preplanned routes can be altered to minimize susceptibility to pop-up threats, which could be previously unknown fixed threats, mobile ground-based threats, or airborne interceptors (see Figure 3).

A rudimentary capability consists of using onboard sensors, e.g., radar warning receivers (RWRs), to detect and derive general locations of emitters of interest, then manually modifying a route segment. A more robust capability would permit

- Full replanning of the entire route, taking into consideration the threat laydown used in preplanning the mission as well as the data collected by onboard and offboard sensors while the aircraft is en route to the target
- Replanning of other attack and support elements of a raid.



(a) Mission planning threat laydown and selected route

(b) Adaptive mission planning threat laydown and adjusted route

Figure 3—Adaptive Route Planning

Before initiating the development of this capability, its effect on the work load of aircrews must be examined.

An adaptive route planning capability is particularly important for coping with relocatable or mobile threats (ground-based air defense systems and airborne interceptors). The locations of ground-based air defenses may change from those used in the penetration analysis performed prior to takeoff. Similarly, the coverage areas of airborne interceptors can change dramatically prior to takeoff. Thus, LO aircraft without an adaptive planning capability run increased risk of flying into the engagement envelopes of potential ground-based threats or into areas covered by airborne interceptors.

Adaptive (or NRT) route planning is a relatively new concept, and it is unlikely that the developers of LO aircraft will provide this capability unless it is listed in the system specifications.

If the survivability of individual cruise missiles becomes important (for whatever reason), an automated form of adaptive route planning could be implemented. For example, pop-up threat detection by an onboard RWR could cause the cruise missile to fly lower to reduce susceptibility to engagement (at the expense of increasing the probability of crashing).

An issue related to adaptive route planning is how to incorporate threat data collected or developed onboard LO aircraft, while en route to target or outbound, into the threat database used for route planning of subsequent missions. This issue is particularly important in environments in which one or a combination of the following conditions is encountered:

- Pop-up threats emerge
- Some anticipated threats do not materialize
- Anticipated locations of known threats change
- Electronic signatures of known threats change.

Without this new information, the threat penetration analysis to support route planning of subsequent strikes is of questionable value. Protocols and procedures should be developed for validating and incorporating threat data collected during mission execution into the route planning of subsequent missions.

4. Implications for the Intelligence Community

This section summarizes the issues surrounding threat penetration analysis and route planning, discussed in the previous sections, within the context of their implications for the intelligence community. Initial steps for addressing some of these issues are also suggested.

Tailored Threat Data

Typically, system specifications for LO programs will include some level of description of the type of threat data that will be provided to developers in support of development and testing. The intelligence community is responsible for providing the threat data to support these programs. In an ideal situation, the data provided by the intelligence community not only meet the requirements of the developers but also are representative of the data that the LO aircraft or cruise missile require for effective employment in diverse operational environments.

Often, instead, tailored and precise threat data that are not representative of operational intelligence data are provided to support developers. If this occurs, the threat analysis and penetration models developed to support mission planning in an operational environment may prove to be inadequate. Thus, it is essential that the Air Force intelligence community ensure that responsible individuals maintain good visibility into how developers use the tailored threat data in developing threat models and penetration models for export to planned operational mission planning systems or possibly to unit-level intelligence support systems. If the tailored and precise threat data are essential for effective employment of LO platforms, then the intelligence community may have to develop the means of providing such data in operational environments. The Air Force TENCAP (Tactical Exploitation of National Capability) program is examining alternatives for providing this capability.

Alternatively, the intelligence community may be able to lessen the developer's reliance on tailored threat data. It could institute a program to better educate the developers and operators about the type of threat information it can actually provide in an environment with major budgetary constraints while coping with

all other demands on national and theater intelligence systems. With a better understanding of the intelligence community's capabilities, developers may be able to build LO platforms and mission planning systems that do not require extensive, tailored threat data.

Operational Threat Data

A review of the Military Integrated Intelligence Data System/Integrated Data Base (MIIDS/IDB), the database that is planned to support mission planning systems, indicates that, because of empty database fields, imprecise data entry, and/or lack of specific fields, it does not provide the following vital information:

- The individual locations of all key elements of a particular defense system, e.g., early-warning radar, acquisition radar, fire control radar, and missile launcher
- The location accuracy of emitters and the source of data
- Information on system characteristics
- The currency of reported data.

As previously discussed, this is the type of threat information that may be required for threat analysis and penetration models to assist aircrews and mission planners in selecting low-risk routes manually or with an autorouter.

The Air Force intelligence community should participate with LO platform and mission planning system developers and operators in

- Defining the need, appropriate use, and specifications for an autorouter for LO aircraft and cruise missiles
- Determining whether populating the various database fields in MIIDS/IDB is sufficient, or if a tailored database must be developed.

Data Security

Most LO platform survivability improvements have been developed under special access programs. Consequently, information important to understanding threat-data requirements is available only to a very small number of intelligence personnel. Conversely, the most accurate and complete threat data available may be classified at a security level (SCI) for which developers may not be cleared. Moreover, some threat databases cannot be released to contractors. Thus, developers may not have visibility into all available threat data, and

cleared intelligence personnel may not have sufficient understanding of LO threat data requirements. Under these conditions, threat penetration models may be developed that prove inadequate.

Developers and intelligence community personnel with the appropriate clearances should establish and maintain an effective dialogue throughout the development and test phases of LO programs. Intelligence Support Working Groups (ISWGs), responsible for developing Intelligence Support Plans (ISPs) for the acquisition of specific LO aircraft and cruise missiles, are good forums for addressing these issues.

Access restrictions to LO aircraft and cruise missile performance models and SCI threat data may also occur in the operational environment. The intelligence and mission planning communities, developers, and operators should develop security protocols and means for allowing the use of the most current and accurate RCS data and the best available threat data in planning routes of LO platforms.

Model Validation

Theoretically and empirically, the physical relationships between low observable technologies, detection methods, and the environment are imprecisely known; such imprecision complicates the development of simple threat models. Because of the complexity of the phenomenologies behind these models and the cost and time required to validate them, the Department of Defense typically does not furnish validated threat models to developers. (We recognize that software developers must differentiate between terms such as *validation, verification,* and *accreditation;* we are not making such a distinction here when we use the term *validation.*)

Thus, LO aircraft and cruise missile developers often must construct their own threat models or modify unvalidated models to test their systems. Clearly, such contractor-developed models may not accurately reflect threat capabilities. The models may be based on

- Inaccurate system performance parameters, such as radar frequency (particularly, war-reserve modes), radar power, and search volume
- Inaccurate response times for LO detection, acquisition, fire control lock-on, and weapon launch
- Modeling assumptions that are inappropriate

Also, the contractors may choose models that require system characteristics data that are either difficult or virtually impossible for the intelligence community to provide. Obviously, if threat models are either inadequate or cannot be supported with available intelligence data, they are of little use to operators.

Problems with threat models may not surface until operational evaluation or until actual deployment of LO platforms. To lessen the probability of this occurrence, the intelligence community, in coordination with the mission planning and system acquisition communities, should, as a minimum, define the level of detail and the spectrum of generic threats that developers must consider in assessing the penetration capabilities of their LO platforms. Such definition should ideally influence the specifications writing process when LO systems are still in Phase 0 of the acquisition process (concept exploration and definition) (Ref. 4). Also, the intelligence community should maintain good visibility into the development of the threat models.

Alternatively, the intelligence community, with substantial support from the mission planning and system acquisition communities, could choose to take on the task of developing, validating, and providing threat models to LO platform developers. The completion of this task would require a substantial investment.

Sentinel Byte/AFMSS Interface

To support unit-level operations, the Air Force intelligence community is developing the intelligence workstation Sentinel Byte (SB). As currently planned, SB Block II is designed to integrate threat data from several sources and prepare files for transfer to the Air Force Mission Support System (AFMSS), the unit-level mission planning system being developed by the Air Force. The primary database to support SB is the MIIDS/IDB; in the future, it will be the Extended Integrated Data Base (XIDB). Using this database, along with threat data developed by theater intelligence assets and threat information collected by units, operations intelligence personnel will create an SB Integrated Data Base. This unit-level database will be the source of threat information for threat and penetration analyses that will be performed on AFMSS. Because of the importance of the SB/AFMSS interface, the Air Force intelligence community must ensure that SB has the right data to support LO aircraft and cruise missiles. The SB database should include data on enemy weapon systems' effectiveness derived from timely HUMINT reports.

Mobile Threats, Airborne Interceptors, and AAA

Mission planning system developers and operators have not defined the procedures for handling mobile threats in threat analysis and penetration models. Conversely, the intelligence community has not defined the procedures for collecting and providing this information in a timely manner to mission planners. Therefore, the Air Force intelligence community should take an active role in

- Assisting LO platform developers and operators in determining whether there is a need for including mobile threats in penetration analysis for LO aircraft and cruise missiles
- If inclusion is deemed necessary, establishing procedures for providing such data in a timely manner to aircrews and cruise missile mission planners.

The intelligence community should also actively participate in discussions with LO platform developers and operators to determine to what extent the modeling of airborne interceptors and AAA should be included in the threat analysis and penetration models to support route selection of LO aircraft and cruise missiles. At a minimum, computer-based decision aids that assist aircrews and mission planners in examining the risk of specific mission profiles to airborne interceptors and AAA should be considered.

Operational Alternatives to Enhance LO Penetration Capabilities

In the near-term, neither SB nor AFMSS will have the capability to evaluate the effects of coordinated aircraft or cruise missile strikes, or the effect of the combination of RCS management and use of onboard or offboard passive and active countermeasures. As a result, aircrews and mission planners will have to evaluate these effects manually. In some cases (e.g., coordinated strikes), such analysis will be done at the force level.

The capability of analyzing coordinated strikes should be incorporated into force-level systems such as the Automated Planning System. As previously discussed, the effective use of such a capability, in addition to RCS management, is important in planning LO missions in a high, overlapping threat environment. The Air Force intelligence community should play an active role by formulating a method of addressing this shortcoming.

Adaptive Route Planning

The development of onboard route modification capabilities would require that NRT threat information be fed to the cockpit of aircraft. To be effective, the intelligence information must fulfill the following three criteria: (1) contain required attributes, (2) be accurate and timely, and (3) be formatted for ease of integration with the onboard aircraft database. Adaptive route planning would also require the development of analytical tools to assess the impact of these adaptive routes on single aircraft and on multiple attack and support aircraft (timing, deconfliction, adapting paths of support aircraft, priorities, etc.).

Because the development of this capability is likely to require a substantial investment, the intelligence community should be pro-active with platform developers and operators in determining the added value of en-route route modifications for LO aircraft. This determination would, in turn, allow the intelligence community to determine the level of effort that should be allocated to populating the MIIDS/IDB fields as compared with improving the quality and accuracy of NRT intelligence data.

References

1. *Interface Control Document for Mission Support System (MSS) Intelligence Data (Draft)*, Air Force Electronic Systems Division, Hanscom AFB, Mass., ESD-82155046A009, 1992.

2. *Mission Planning Operator's Manual for the Tactical Aircraft Mission Planning System (TAMPS)*, McDonnell Douglas Corporation, St. Louis, Mo., October 1, 1990.

3. Discussions with Neil Meeks on mission planning systems, McDonnell Douglas Missile Systems Company, St. Louis, Mo., 1992.

4. *Defense Acquisition Management Policies and Procedures*. DoD Instruction 5000.2, Office, Under Secretary of Defense for Acquisition, Washington, D.C., February 23, 1991.